[Insert Cover Picture]

Chemical Sector Active Threat Tabletop Exercise

Situation Manual

[Insert Date]

[Insert Caveat]

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is

Photo Courtesy of [insert source]

intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

Exercise Agenda

Start Time	End Time	Activity
7:45 a.m.	8:30 a.m.	Registration
8:30 a.m.	8:45 a.m.	Welcome and Participant Briefing
8:45 a.m.	9:45 a.m.	Module One: Incident and Response
9:45 a.m.	9:55 a.m.	Break
9:55 a.m.	10:55 a.m.	Module Two: Sustained Response
10:55 a.m.	11:05 a.m.	Break
11:05 a.m.	12:05 p.m.	Module Three: Short-Term Recovery
12:05 p.m.	12:30 p.m.	Hot Wash

**All times are approximate*

This page is intentionally left blank.

Exercise Overview

Exercise Name	Chemical Sector Active Threat Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX, planned for [insert exercise duration], and will focus on [insert scope]. This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [select appropriate Mission Areas]
Capabilities	Economic Recovery; Mass Care Services; On-Scene Security, Protection, and Law Enforcement; Operational Communications; Operational Coordination; Planning; Public Health, Healthcare, and Emergency Medical Services (EMS); and, Public Health Information and Warning [insert other core capabilities]
Objectives	1. Review emergency preparedness plans and response procedures for a [insert threat vector] at a chemical sector facility. 2. Discuss the coordination between private sector organizations and responding local, state, and federal agencies under the National Incident Management System (NIMS). 3. Assess procedures for coordinating and sharing information within organizations, between organizations, and with the public. 4. Review organizational interdependencies and recovery plans. 5. [Insert additional exercise objectives as necessary]
Threat or Hazard	Active Shooter, Complex Coordinated Attack, Edged Weapon, Improvised Explosive Device (IED), Vehicle-Borne Improvised Explosive Device (VBIED), and Vehicle Ramming. [Insert additional threat vector, as necessary]

Scenario	An interactive, discussion-based exercise focused on an attack on a chemical sector facility. The scenario consists of three modules: Incident and Response, Sustained Response, and Short-Term Recovery.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable]
Participating Organizations	[Please see Appendix A.]
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor).]

General Information

Exercise Objectives and Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

For additional information regarding core capabilities, please visit:

https://www.fema.gov/emergency-managers/national-preparedness/mission-core-capabilities.

Exercise Objectives	Capability
Review emergency preparedness plans and response procedures to a [insert additional threat vector] at a chemical sector facility.	✓ Mass Care Services ✓ On-Scene Security, Protection, and Law Enforcement ✓ Operational Communications ✓ Operational Coordination ✓ Planning ✓ Public Health, Healthcare, and EMS ✓ Public Information and Warning
Discuss the coordination between private sector organizations and responding local, state, and federal agencies under NIMS	✓ Planning ✓ Operational Coordination
Assess procedures for coordinating the sharing information within organizations, between organizations, and with the public.	✓ Planning ✓ Public Information and Warning ✓ Operational Coordination ✓ Operational Communications
Review organizational interdependencies and recovery plans.	✓ Planning ✓ Operational Coordination ✓ Economic Recovery
[Insert objective]	✓ [Insert capability aligned to each objective]

Table 1. Exercise Objectives and Associated Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers:** Do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitator:** Provides situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Moderators:** Moderators are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
- **Evaluators:** Are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

- Module One: Incident and Response
- Module Two: Sustained Response
- Module Three: Short-Term Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission areas] issues.

Exercise Guidelines

- This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.

- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your jurisdiction's/ organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission areas] efforts. Problem-solving efforts should be the focus.
- The assumption is that the exercise scenario is plausible and events occur as they are presented. All players will receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

Module One: Incident and Response

Scenario

[Insert Location]

[Insert Month, Day, Year]: [Time]

[Insert your vehicle service provider] reports a stolen vehicle to the police department. A case was opened to search for the missing vehicle, though neither the company nor law enforcement have a potential lead to follow.

[Insert Date + 1 Day]: [Time]

[Option 1: Active Shooter]

[Insert your facility name] is busy as usual. Several deliveries are expected today, and a couple of shipments have already arrived. In the early afternoon, a familiar truck pulls up to the loading dock. After the truck comes to a stop, there is a brief pause as the driver of the truck staggers out in tactical gear with a rifle in his hand.

He begins firing at employees and forces his way onto the delivery platform as he continues to shoot. Bystanders instinctively disperse away from the dock, with a few victims seeking out security personnel to provide varying accounts of the shooter. Before the suspect reaches the door for entry into the facility, he is cornered by responding officers and kills himself.

[Option 2: Complex Coordinated Attack (Active Shooter / IED)]

[Insert your facility name] is busy as usual. Several deliveries are expected today, and a couple of shipments have already arrived. In the early afternoon, a familiar truck pulls up to the loading dock. After the truck comes to a stop, there is a brief pause as the driver of the truck staggers out in tactical gear with a rifle in his hand.

He begins firing at employees and forces his way onto the delivery platform as he continues to shoot at bystanders. As the assailant moves towards the door that permits entry to the inside of the building, responding officers begin to return fire. The shooter continues to take shots, but much more sporadically.

Officers examine the outside of the facility in which the shooter is cornered, and observe the shooter's crashed truck near the dock, where a number of people lie apparently dead or injured in the truck's path, before noticing an object in the truck bed that looks like a large IED.

[Option 3: Edged Weapon]

[Insert your facility name] is expecting several deliveries today. At 1:30 p.m., a familiar truck slowly pulls up to the loading dock. After it comes to a

stop, there is a brief pause as the driver of the truck staggers out carrying a machete. He begins slashing at nearby employees around the facility and forces his way onto the delivery platform. He continues to slash people until he is confronted by responding officers and is fatally wounded while rushing them.

[Option 4: IED]

[Insert your facility name] is busy as usual. Several deliveries are expected today, and a couple of shipments have arrived already. An employee notices an unmarked package sitting inside the entrance of the loading dock and proceeds to pick it up. Suddenly, the package detonates, and a large explosion occurs inside the loading dock. Bystanders are thrown back and struck by flying debris from the blast.

Many employees who were in the facility at the time of the attack were able to escape through emergency fire exits, but they report that there are more seriously injured people still inside. Several victims seek out first responders and indicate that they could hear people calling out from the direction of the loading dock, but they could not see anyone through the dark smoke, dust, and rubble.

[Option 5: VBIED]

[Insert your facility name] is busy as usual. Several deliveries are expected today, and a couple of shipments have already arrived. Another truck is pulling into the loading dock when the vehicle suddenly accelerates and veers sharply to the right, over the curb, through employees, and directly into the dock, where it explodes. Bystanders are thrown back and struck by flying debris from the blast.

Many employees who were in the facility at the time of the attack were able to escape through emergency fire exits, but they report that there are more seriously injured people still inside. Several victims seek out first responders and indicate that they could hear people calling out from the direction of the shattered lobby, but they could not see anyone through the dark smoke, dust, and rubble.

[Option 6: Vehicle Ramming]

[Insert your facility name] is busy as usual. Due to the increased demand of [insert your facility's products / services], there was an uptick of shipments and deliveries to and from the facility. Dozens of shipments have already arrived today, with several more still expected. At [insert time of day], another truck pulls into the loading dock when the vehicle suddenly accelerates and veers sharply through employees. The truck reverses aimlessly, before accelerating into a group of bystanders again and colliding directly with the dock.

The driver of the vehicle staggers out of the truck with a knife. As he charges forward with the weapon in his hand, the assailant is confronted by responding officers.

Discussion Questions

1. What plans are in place to prevent or deter an attack at your facility?
    a. What threats are you most concerned with preventing?
    b. Who is responsible for the security plan and necessary updates?
    c. Are multiple agencies outside of your organization involved in the response and recovery planning process?
    d. What plans / deterrents are in place to deter / prevent a vehicle intrusion (i.e., barricades, traffic control)?
    e. What plans / deterrents are in place to deter / prevent an active shooter (i.e., screening, security presence)? [Option 1]
    f. What plans / deterrents are in place to deter / prevent an IED (i.e., screening, canine teams)? [Option 2]
2. How are security and personnel trained?
    a. What training programs are in place for personnel? Who trains them?
    b. How are personnel trained to respond to a vehicle intrusion?
    c. How are personnel trained to respond to an active shooter? [Option 1]
    d. How are personnel trained to respond to an IED? [Options 2 or 4]
    e. What are the rules of engagement for your security personnel?
    f. What is the chain of command for onsite security personnel?
    g. Have security personnel had the opportunity to coordinate with local law enforcement?
    h. Which organizations contribute to the security of your facility?
3. Does your organization's standard operating procedures (SOPs) include incident response roles and responsibilities for staff?
4. What assets are onsite to immediately respond to an incident?
    a. What resources are available that would help with response?
5. What additional offsite capabilities are available to respond to your facility?
    a. What law enforcement assets are available to respond?

b. What emergency medical services (EMS) assets are available to respond?
c. What emergency management agencies are able to support this incident?
d. Are there volunteer organizations or other partner groups that would have resources that would participate in the immediate response, such as the Red Cross?

6. What notification methods (e.g., alerts, emails, telecommunications, text messages, special tools) does your facility use to send alert information?
   a. Who is responsible for sending out the alerts or warnings? Does your facility utilize Public Information Officers (PIOs)?
   b. Are there pre-built templates for different incidents?
   c. What protocols are in place for alerting employees to an incident?
   d. What protocols are in place for notifying authorities of the incident and how are any first responders notified?
   e. Do you have protocols in place for alerting partner organizations to an incident?
   f. If the cell network is overwhelmed, does that affect your warning procedures?
   g. Are there alternate alter methods?
   h. What partner agency would alert nearby residents / businesses / schools if a shelter-in-place or lockdown procedure needs to be implemented?
7. What does incident command look like during this phase of the response?
   a. Do you have an identified Incident Command Structure?
   b. How is incident command approached by each of the relevant agencies, and what would it look like in the opening minutes of the incident?
   c. At what point would you expect incident command to formalize?
   d. When would you expect unified command to begin coming together?
   e. Are key agencies and facility personnel familiar with the Incident Command System (ICS)?
   f. What are each organizations' priorities at this stage of the incident?
   g. What mutual aid agreements are in place to assist in the response to an incident?

8. How would law enforcement conduct the response and address the threat?
    a. Which local and / or federal law enforcement agencies are involved?
    b. Which agency would have the lead?
    c. How would law enforcement respond to the reports of a vehicle intrusion attack?
    d. How would the response change when it became a(n) [edged-weapon attack / active shooter] situation?
    e. How would the response change when the IED was spotted? [Option 2]
    f. Are there any additional agencies or resources needed to address an IED? [Option 2]
    g. Are there any law enforcement SOPs that would affect other entities (i.e., moving Fire / EMS out of an IED blast radius after the explosive is discovered, or potentially taking over nearby businesses for command posts or sniper positions)?
    h. How would you resolve the situation?
    i. Are local law enforcement officers familiar with [insert your facility name] and its schematics?
9. How would the medical response be conducted?
    a. Does [insert your facility name] have a medical cadre trained to respond to this kind of event?
    b. Which organizations and agencies are involved?
    c. Which organization or agency would have the lead?
    d. Is there a Mass Casualty Plan in place for this event? Does [insert your facility name] have plans for specific incidents?
    e. At what point would the hospitals be informed of the incident?
        i. Who is responsible for contacting the hospitals?
    f. At what point would first responders' protocols allow medical personnel to enter the scene and begin triage and treatment of the injured?
        i. What challenges would the ongoing evacuation procedures pose?
        ii. What actions, if any, would EMS personnel be able to take while the shooter is still active?

iii. What actions, if any, would EMS personnel be able to take once an IED had been identified? [Option 2]

iv. What are EMS agencies' procedures regarding entry into a warm zone?

v. Do your EMS agencies have protective gear and training for tactical entry?

10. What information or warnings are being released to the public?

a. Who is responsible for the initial messaging?

b. How quickly is information being released?

c. What methods are being used to distribute information?

d. What should the content of the messaging be?

e. Is targeted information sent to businesses or people in the surrounding area?

f. Do you send out any notifications to the public using social media? If so, at what point in the incident would you expect to start sending the notifications?

g. Are other participating organizations (i.e. law enforcement, fire department, EMS, etc.) providing their own messaging to their employees?

i. How is the information obtained?

ii. How is the information distributed?

iii. Who in your organization is responsible for this?

iv. Are there pre-built templates for different incidents?

h. When would a Joint Information Center (JIC) be activated?

i. How are messages coordinated across the different agencies and organizations before the JIC is activated?

11. If your organization or agency received information of a potential threat prior to the day of the incident taking place, what mitigation procedures would have taken place?

a. How would those mitigation procedures have influenced the response if the attack had still occurred?

b. Do your agencies and organizations cross-train on various attack scenarios?

c. How would you prevent or protect against this type of attack happening at your facility?

d. What additional measures would you put in place to secure your dangerous chemicals?

12. What are your evacuation procedures for an incident of this type?
    a. Are there plans in place for a mass evacuation?
        i. Who is responsible for activating evacuation procedures?
        ii. Is there a specified rally point for evacuees?
        iii. Would this location be impacted by weather?
        iv. Are there secondary and tertiary rally points in case the primary point is a part of the incident or overwhelmed by evacuees?
    b. Are there plans in place if the situation warrants shelter-in-place?
    c. What plans or procedures are in place to work with access and functional needs populations?
    d. Would there be any accountability taken of employees and, if so, how is it accomplished?
13. Given the scenario, does your Emergency Action Plan (EAP) include measures for protecting the security of chemicals at your facility?
    a. Do you have plans to maintain control of the chemicals in the event of an evacuation and / or do you plan to do an inventory check after the event?
    b. Will you need to pause operations during an evacuation?
14. Who is responsible for ensuring the chemical security measures are met?
15. Given the scenario, does your notification to responders include information about the chemicals at your facility?
    a. Do you maintain a relationship with first responders as to what chemicals are at your facility?
    b. Do you know if they are able to adequately respond if an attack at your facility impacts those chemicals?
    c. Who else within the first responder community should be notified if the attack impacts those chemicals?

Module Two: Sustained Response

Scenario

[Insert Location]

Afternoon, [Insert Day of Week] [Month, Day, Year]: [Time]

After the assailant is neutralized [If Option 2 is chosen, add: "and the IED is rendered safe"], EMS personnel rush in to triage the wounded. The attack left [insert number] people killed and [insert number] people wounded, with [insert number] of those in critical condition. [Insert jurisdiction] Fire and EMS have already called in their mutual aid partners from surrounding jurisdictions, and ambulances are beginning to arrive on the scene. In addition, [insert jurisdiction] police officers securing the scene reported that several neighboring law enforcement agencies from different parts of the state have offered their aid.

Media is arriving on the scene and is attempting to interview witnesses and first responders. The mayor arranges for a media briefing later that afternoon.

Evening, [Insert Day of Week] [Month, Day, Year]: [Time]

Early in the evening, the governor calls to express his condolences and detail what the state is doing to respond. Shortly thereafter, representatives of state and federal agencies begin to arrive on scene. At the press conference, the mayor expresses his grief and outlines to reporters from across the nation what steps the city is taking to manage the incident. The motivation of the attacker is not yet known.

Discussion Questions

1. What command structure would be setup for the incident and how would it evolve over the course of the afternoon and evening?
    a. Which agencies would be involved in unified command?
    b. At what point would the emergency operations center (EOC) be stood up?
        i. What agencies and organizations will be in the EOC?
    c. What is the role of private sector stakeholders in this command structure?
    d. In addition to unified command, which agencies would have their own command centers setup in other locations?

e. How would the EOC interface with unified command (phones radios, liaisons, etc.) and how would participants define their roles?

f. Would a Multi-Agency Coordination (MAC) Group be stood up and, if so, when?

   i. How would you define the role of a MAC Group in a situation such as this?

   ii. How would this MAC Group coordinate and interface with other command and control structures?

g. How would arriving mutual aid agencies integrate into the command structure and at which locations (unified command at scene, EOC, hospital, etc.)?

   i. Are they trained on incident command procedures?

   ii. Is there cross-training with public agencies on the private sector's incident priorities?

2. What communication methods (e.g. alerts, emails, telecommunications, text messages, and special tools) does your facility and other private sector organizations use to share information?

   a. Does your facility's communication structure remain the same throughout the incident or does it change or modify as the incident evolves?

   b. How does your organization communicate with first responders?

   c. What other private sector organizations would you communicate with?

   d. What communication methods would you use for coordinating with your private sector partners?

   e. Who in your organization is responsible for communication during an incident?

   f. What alternate communication procedures exist?

   g. Do you use social media to communicate with the public? If so:

      i. At what point in the incident would this begin?

      ii. Who in your organization would be responsible for this function during an incident?

3. What communication methods (e.g., alerts, emails, telecommunications, text messages, and special tools) do first responders use to share information with other responders?

a. What communication methods do local first response agencies use to communicate with their local counterparts (i.e. how do police officers communicate with fire or medical personnel)?
b. What communication methods do local first response agencies use to communicate with their respective mutual aid partners?
c. How are communications coordinated when multiple response agencies from multiple jurisdictions are on scene? Who is responsible for this communication?
d. How do you communicate with the private sector?
e. If the cell network is overwhelmed, does that affect your communication procedures?
f. Are there alternate communication procedures?
g. Do you use social media to communicate with the public? If so:
    i. At what point in the incident would this begin?
    ii. Who in your organization would be responsible for this function during an incident?

4. What are your organization's information sharing responsibilities at this point in an incident?
    a. What formal information sharing processes would your organization use at this point?
    b. What resources are used to disseminate information?
    c. Who would be responsible for messaging in your organization?
        i. Would your messaging be coordinated with any other organizations and, if so, how?
    d. How would you send information to your employees?
    e. How would you send information to your patrons or customers (if applicable)?
    f. Who is responsible for communicating information to family members of those killed or injured?
    g. Who is responsible for communicating information to potentially impacted businesses?
    h. What are your communication goals?
5. Who is in charge of notifying state or federal agencies of the incident, and at what point in the incident would this occur?
    a. What resources or actions would you expect from state or federal agencies?

   b. How would arriving state and federal resources integrate into the command structure and at which locations (unified command, area command, EOC, MAC Group etc.)?

6. What role do city and county governments play in this scenario?
   a. Who is responsible for informing the mayor, county commissioners, or other local elected officials?
   b. Have protocols been established with elected officials so that they know what to expect during incident response? Do local agencies know what elected officials' priorities are?
   c. Is there a location, such as the EOC, where elected officials will know to go during an incident?
      i. If so, where is it?
   d. Have elected officials been briefed on ICS?
   e. What support from first response agencies would the mayor or county commissioner expect in holding a press conference on the incident?
      i. What information would be needed at the press conference?
      ii. Would law enforcement be required to provide security at the press conference?
      iii. Would the mayor or county commissioner expect department chiefs to attend the conference?
7. Does your organization have a designated PIO? If so:
   a. Are protocols in place for addressing media inquiries?
   b. How do they receive information from the incident?
   c. Do they have pre-built public information templates for use in different kinds of emergencies?
   d. Would your organization use social media during an incident?
8. Would mass care facilities, family assistance, or reunification centers be setup? If so:
   a. At what point in time?
   b. Which agencies are involved, and who is responsible for leading this aspect?
   c. What procedures are in place?
   d. Which facilities would be used?
   e. How are victims and family members made aware of the location?

f. Which agency or person, if any, would be in charge of setting up these facilities?

9. What is your agency's protocol for addressing self-dispatching responders?
   a. Does it differ based on whether the help is offered in the initial moments of the attack, as opposed to later in the incident?
   b. Is the protocol the same for law enforcement as it is for EMS?
10. If this were to be declared a terrorist incident, what impact would that have? Would this impact the response, recovery, or both?
   a. How would that impact state and federal involvement?
   b. If the attacker were determined to be backed by a terrorist organization (as opposed to a lone wolf inspired by a terrorist organization) what impact would that have?
11. What steps are needed to ensure the area is cleared of threats?
12. What is the process to collect evidence that belongs to citizens (cell phone video, cameras, security footage from private businesses, etc.)?
13. How are personal items reunified with their owner if left at the scene?
14. What are some of your agency's best practices for response?
15. Following this attack, what additional protective measures will be put into place at your organization or in your community?
   a. How would information on protective measures be obtained?
   b. How would any relevant classified information be shared?
   c. How is relevant information shared within your critical infrastructure sector?
      i. How do you communicate information to other members of your sector or receive information from them?
      ii. Do you know how to contact your Sector-Specific Agency (SSA)?
      iii. Do you have a Homeland Security Information Network – Critical Infrastructure (HSIN-CI) account and are you able to use it?
   d. Do you know how to contact your CISA Protective Security Advisor (PSA)?
   e. If you are a regulated facility, do you have points of contact and their contact information?

MODULE THREE: SHORT-TERM RECOVERY

Scenario

[Insert Location]

[Insert Month, Day, Year]: [Time]

The investigation is still ongoing several days later, but it is clear that the assailant acted alone. Police continue to investigate the assailant's connection to the facility. Local media is asking how [insert your facility name] will respond and what measures will be taken to ensure such an attack does not take place again.

Initial reports show that there was significant loss of equipment, financial resources, and supplies in the attack. Local businesses based in the impacted area are asking officials when they can reopen and resume normal operations. The [Insert locality] Chamber of Commerce is asking what state and federal grants can be provided to help the city recover.

Families of those who lost their lives in the attack have contacted the mayor's office to ask for police escorts for the funeral processions, as well as to ask what sort of city memorial events are planned. National attention continues to be focused on the community and the press is expected to try to cover the funerals and memorial services.

Discussion Questions

1. Does your organization have a business continuity or rapid recovery plan?
    a. Do these plans include a crisis communications plan?
        i. How and what type of messaging will be sent to employees, vendors, and customers?
        ii. What training do employees receive regarding media relations and the release of sensitive information?
    b. What are the short-term recovery objectives for your organization?
    c. What are the implications of being unable to open or operate for a period of time?
        i. Given the scenario, how long would the incident area remain cordoned off for the investigation?
        ii. What would the financial impact be on your organization if your building was closed due to such an incident and the ensuing investigation?

iii. Would your business close as a result of this incident, even if it did not directly impact you?

iv. How would you ensure the security of your dangerous chemicals?

v. Are there any mandatory actions for chemical maintenance that must be continuously performed?

vi. Are personnel available and will they have access to monitor / inspect your chemical storage area?

d. Does your organization have the ability to move key operations to another location?

i. If so, how long would this take?

ii. If operations are moved to another location, can your chemicals be safely relocated?

e. Do you have any insurance that would assist given this scenario?

i. If the incident had been declared terrorism, would this impact insurance?

f. What training plans are in place for the business continuity plan? Does your organization exercise these plans (other than today)?

2. What types of information are needed to assist in restoration of your organization's critical infrastructure?

a. What information would your organization expect to receive? How does your organization expect to receive this information and from whom?

b. What information would your organization expect to provide to those organizations that could assist with your return to full operations?

c. How would your organization expect to provide information and to whom?

3. How can owners / operators and government officials prepare to handle the public messaging / media in the aftermath of such an incident?

a. Does your media plan include incidents such as this?

b. Have your PIOs had the opportunity to collaborate with other supporting organizations' PIOs during a crisis

c. What is the plan to handle the significant media attention from national and international outlets?

d. How will you restore public confidence?

e. How will you resolve potential misinformation?

f. How will you respond to media requests (written notices, press conferences, interviews, etc.)?

g. Is social media being monitored to maintain awareness of information spreading that may not be accurate?

   i. Who is responsible for monitoring social media?

   ii. What procedures are in place to counter false information on social media?

4. Given the scenario, what measures would be needed to support your organization's employees following this incident?

   a. How is information communicated to employees during the days following the incident?

   b. Would leave or time-off be granted to employees?

   c. If operations are suspended for a length of time, is there financial assistance available to employees?

   d. Are there any additional security measures that you put into place following this event?

   e. How do you reassure employees as to their safety on the job?

   f. Are there plans in place to provide emotional counseling to those employees and family members traumatized by the attack?

   g. If some of your employees were killed or injured in the attack, how would it change your actions?

      i. Is there assistance available for injured employees? If so, what kind (counseling, monetary, legal, etc.)?

      ii. Is there assistance available for the families of those employees who were killed? If so, what kind (counseling, monetary, legal, etc.)?

      iii. How would the loss of personnel impact your operations? What steps might be taken to adjust for, or mitigate this?

5. What resources are available to assist your facility or organization with recovery?

   a. Are pre-arranged agreements in place to obtain key resources?

   b. If so, how are these agreements activated (i.e., what type of coordination and request process is required)?

   c. Would your organization or state / local organizations be requesting grant assistance to support recovery efforts?

6. What are your facility or organization's interdependencies?

a. What stakeholders are dependent upon your organization and its services?
b. Who are the key stakeholders or groups that your organization relies upon to help restore your operations and assets?
c. What private sector organizations / resources do public sector organizations rely on to help restore mission essential functions?
d. What public sector organizations / resources do private sector organizations rely on to help restore critical infrastructure assets?
e. Do you have contracts / agreements in place with the organizations that control / own these resources / services for priority services in an emergency?
f. Who are the key mobilizers or champions (either individuals or functional roles) in your organization or community who must be engaged for an effective recovery?

7. What is the community's plan to recover?
   a. Is there a formal recovery plan and, if so, does it cover this type of incident?
   b. Will there be a memorial event held in the community, and which organizations would take the lead in organizing it?
   c. What assistance would you look for from volunteer, community, or faith-based organizations?
   d. What would your organization do to support recovery in the community?
   e. What assistance would city agencies provide to private sector organizations?
   f. What assistance would you request or expect from the state government?
   g. What assistance would you request or expect from the federal government?
   h. Are there contracts in place to assist in the cleanup and recovery prior to reopening your facility?
   i. Are there any additional measures that law enforcement would take to ensure the safety of the community or to reassure citizens?
      i. How would these measured be resources?
   j. Who makes the decision on when the area will be reopened?
      i. How is that decision communicated to the public and the media?

k. At what point would you consider the recovery complete?

8. Are there best practices for recovery that you would like to share?

APPENDIX A: EXERCISE PARTICIPANTS

Participating Private Sector Organizations
[Insert private sector participants]

Participating Local Organizations
[Insert local participants]

Participating State Organizations
[Insert state participants]

Participating Federal Organizations
[Insert federal participants]

Other Participating Organizations
[Insert other participants]

Other Participating Organizations

This page was intentionally left blank.

APPENDIX B: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX C: ACRONYMS

Acronym	Term
AAR	After-Action Report
CFATS	Chemical Facility Anti-Terrorism Standards
CISA	Cybersecurity and Infrastructure Security Agency
COI	Chemicals of Interest
CTEP	CISA Tabletop Exercise Package
CSI	Chemical Security Inspector
EAP	Emergency Action Plan
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EPT	Exercise Planning Team
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
ICS	Incident Command System
IED	Improvised Explosive Device
IP	Improvement Plan
JIC	Joint Information Center
MAC	Multi-Agency Coordination
NGO	Non-Governmental Organization
NIMS	National Incident Management System
PIO	Public Information Officer
POC	Point of Contact
PSA	Protective Security Advisor
SitMan	Situation Manual
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SSA	Sector-Specific Agency
TTX	Tabletop Exercise
VBIED	Vehicle-Borne Improvised Explosive Device

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY